(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 847 031 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
10.06.1998 Patentblatt 1998/24

(51) Int. Cl.[6]: G07F 7/10

(21) Anmeldenummer: 97119367.7

(22) Anmeldetag: 05.11.1997

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: 05.12.1996 DE 19650549

(71) Anmelder:
ODS R. Oldenbourg Datensysteme GmbH & Co. KG
85375 Neufahrn (DE)

(72) Erfinder:
- Lohmer, Reinhard
  83052 Bruckmühl (DE)
- Ness, Werner
  85716 Unterschleissheim (DE)
- Muth, Ralf-Jürgen
  83620 Feldkirchen-Westerham (DE)

(74) Vertreter:
Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) Verfahren zum gesicherten nachträglichen Programmieren einer Mikroprozessorkarte für eine zusätzliche Anwendung

(57) Verfahren zum nachträglichen Programmieren einer Mikroprozessorkarte für ein zusätzliche Anwendung, mit folgenden Schritten: Speichern eines Schlüssels K in einem Speicher der nachträglich zu programmierenden Mikroprozessorkarte, Erstellen einer Befehlssequenz, mittels der die Mikroprozessorkarte für die zusätzliche Anwendung konfigurierbar ist, Verschlüsseln der Befehlssequenz derart, daß die Befehlssequenz mittels des Schlüssels K entschlüsselbar ist, Speichern der verschlüsselten Befehlssequenz auf einem Datenträger, vorzugsweise einer weiteren Mikroprozessorkarte, Einrichten einer Datenkommunikation zwischen der nachträglich zu programmierenden Mikroprozessorkarte und dem Datenträger bzw. der weiteren Mikroprozessorkarte, Durchführen eines Authentisierungsverfahrens zum Überprüfen, ob die nachträglich zu programmierende Mikroprozessorkarte für die nachträgliche Programmierung zugelassen ist, und/oder ob der Datenträger bzw. die zusätzliche Mikroprozessorkarte für die nachträgliche Programmierung zugelassen ist, bei erfolgreichem Abschluß der Authentisierung schrittweises oder vollständiges Übertragen der verschlüsselten Befehlssequenz von dem Datenträger bzw. der weiteren Mikroprozessorkarte an die nachträglich zu programmierende Mikroprozessorkarte, Entschlüsseln der empfangenen, verschlüsselten Befehlssequenz bzw. Befehlssequenzteile durch den Mikroprozessor der zu programmierenden Mikroprozessorkarte mittels des gespeicherten Schlüssels K, Anlegen von Datenstrukturen innerhalb eines freien Speicherbereiches der nachträglich zu programmierenden Mikroprozessorkarte entsprechend der Befehlssequenz, wodurch die Mikroprozessorkarte für die zusätzliche Anwendung konfiguriert wird.

EP 0 847 031 A1

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren zum gesicherten nachträglichen Programmieren einer Mikroprozessorkarte für eine zusätzliche Anwendung.

Ein Hauptanwendungsgebiet für moderne Mikroprozessorkarten liegt im Bankenbereich, wobei hier insbesondere, Anwendungen zum Durchführen von Geldtransaktionen als auch zur Verwendung als elektronische Börse eine Rolle spielen.

Mikroprozessorkarten weisen neben einer CPU, einem RAM und einem ROM üblicherweise einen zusätzlichen Datenspeicher, vorzugsweise ein EEPROM, auf, das im Rahmen der Personalisierung der Karte anwendungsspezifisch beschrieben wird. Dieser spezielle Speicherbereich ist üblicherweise so groß bemessen, daß nach der Konfigurierung der Karte für die Hauptanwendung noch Platz für weitere Anwendungen verbleibt.

Derartige weitere Anwendungen können beispielsweise in der Verwendung der Karte als Identifikationsmittel (elektronischer Fahrschein) im öffentlichen Beförderungsverkehr, als Träger von speziellen Kundendaten für Handelsketten (z.B. Bonussysteme) etc. liegen.

Um eine Mikroprozessorkarte, die originär für den Bankenbereich ausgegeben wurde, auch für derartige zusätzliche Anwendungen benutzen zu können, ist eine entsprechende Konfigurierung der Karte erforderlich. Hierzu wurde bereits vorgeschlagen, den erwähnten freien Speicherbereich bereits bei der ursprünglichen Programmierung der Karte für eine Anzahl zusätzlicher Anwendungen aufzuteilen, und bereits die für die Anwendungen notwendigen Datenstrukturen anzulegen. Um die entsprechende Karte später für eine derartige Anwendung verwenden zu können, ist noch ein "Freischalten" des entsprechend vorkonfigurierten Bereiches auf der Karte notwendig, was beispielsweise durch eine Schlüsselabfrage erfolgen kann.

Nachteilig an dieser bekannten Vorgehensweise ist die unflexible Aufteilung des für die zusätzlichen Anwendungen zur Verfügung stehenden Speicherbereiches, wodurch sich keine anwendungsspezifische optimale Aufteilung und somit optimale Benutzung des zur Verfügung stehenden Speicherplatzes erreichen läßt.

Es ist die Aufgabe der vorliegenden Erfindung, ein Verfahren anzugeben, mit dem Mikroprozessorkarten in flexibler und abgesicherter Weise nach ihrer Ausgabe an die Kunden für zusätzliche Anwendungen auch von Dritten konfiguriert werden können.

Diese Aufgabe wird durch den Gegenstand des Patentanspruches 1 gelöst.

Bevorzugte Ausgestaltungen der Erfindung sind Gegenstand der Unteransprüche.

Die vorliegende Erfindung baut auf der Erkenntnis auf, daß es nachteilhaft ist, den auf einer Mikroprozessorkarte für zusätzliche Anwendungen zur Verfügung stehenden freien Speicherplatz bereits während der ursprünglichen Initialisierung oder Personalisierung der Karte in vorbestimmte Felder aufzuteilen, unter Umständen bereits mit bestimmten Datenstrukturen zu beschreiben und die entsprechend vorkonfigurierten Bereiche später einzelnen Anwendungen zuzuweisen.

Gemäß der vorliegenden Erfindung ist eine Vorstrukturierung des freien Speicherbereiches nicht erforderlich, die Anpassung der Mikroprozessorkarte an eine zusätzliche Anwendung kann nachträglich noch zu dem Zeitpunkt erfolgen, zu dem entschieden wird, daß die Karte für eine zusätzliche Anwendung verwendet werden soll.

Im folgenden wird eine bevorzugte Ausführungsform des erfindungsgemäßen Verfahrens beschrieben.

In einen Speicherbereich der Mikroprozessorkarte, die beispielsweise von einem Kreditinstitut ausgegeben wird, wird während der ursprünglichen Personalisierung oder Initialisierung ein Schlüssel K eingeschrieben, der vorzugsweise, aber nicht notwendigerweise, allen Karten, die von dem entsprechenden Kreditinstitut ausgegeben werden, gemeinsam ist. Die fertig personalisierte Karte weist bei ihrer Ausgabe an den Kunden innerhalb eines beschreibbaren Speichers, vorzugsweise eines EEPROMS, einen für zusätzliche Anwendungen geeigneten freien Speicherbereich auf, der zum gegenwärtigen Entwicklungsstand beispielsweise einige Kilobyte groß sein kann, bei zukünftigen Chipgenerationen jedoch auch erheblich größer ausfallen kann.

Entschließt sich der Kunde zu einem späteren Zeitpunkt, die Mikroprozessorkarte für eine weitere Anwendung zu verwenden, beispielsweise als Zahlungsmittel für ein Transportunternehmen oder eine Handelskette, so kann er die Karte bei einer geeigneten Stelle, vorzugsweise bei dem Unternehmen selbst, auf das die Anwendung zugeschnitten ist, entsprechend nachprogrammieren lassen.

Die entsprechende Stelle verfügt über einen Datenträger, auf dem eine Befehlssequenz gespeichert ist, mittels der der Mikroprozessor veranlaßt werden kann, in einem geeigneten Teil des freien Speicherbereiches Datenstrukturen anzulegen, durch die die Mikroprozessorkarte für die entsprechende zusätzliche Anwendung konfiguriert wird.

Die auf den Datenträger der entsprechenden Stelle vorhandene Befehlssequenz muß somit an den Mikroprozessor der Karte übertragen werden, damit der Mikroprozessor die entsprechende Konfigurierung vornimmt. Aus Sicherheitsgründen muß die entsprechende Programmsequenz auf geeignete Weise abgesichert, z.B. verschlüsselt zur Mikroprozessorkarte übertragen werden, wobei die Mikroprozessorkarte mittels dem vorgespeicherten Schlüssel K in der Lage ist, die Befehlssequenz zu entschlüsseln.

Darüber hinaus erfolgt vorzugsweise vor der eigentlichen Datenübertragung eine Authentisierung, bei der festgestellt wird, ob die entsprechende Stelle berechtigt ist, eine Umprogrammierung der Mikroprozessorkarte durchzuführen und/oder bei der festgestellt wird, ob die

Mikroprozessorkarte berechtigt ist, entsprechend umprogrammiert zu werden. Vorzugsweise erfolgt die Authentisierung entsprechend bekannter Verfahren unter Einbeziehung des in der Mikroprozessorkarte für die Entschlüsselung abgelegten Schlüssels K.

Die Übertragung der Befehlssequenz von dem bei der erwähnten Stelle vorhandenen Datenträger zur Mikroprozessorkarte hin erfolgt vorzugsweise unter Zwischenschaltung eines geeigneten Terminals, in das die nachzukonfigurierende Mikroprozessorkarte eingesteckt wird. Vorzugsweise besteht der Datenträger, auf dem die Befehlssequenz gespeichert ist, ebenfalls aus einer Mikroprozessorkarte und enthält die Befehlssequenz bereits in verschlüsselter Form. Somit ist denkbar, daß Filialen einer bestimmten Handelskette jeweils im Besitz einer derartigen "Trägerkarte" sind und durch die auf der Trägerkarte verschlüsselt gespeicherte Befehlssequenz mittels eines geeigneten Terminals auf eine entsprechende Mikroprozessorkarte übertragen wird. Ein entsprechend geeignetes Gerät könnte somit sowohl einen Aufnahmebereich für die Trägerkarte als auch einen Aufnahmebereich für die Kundenkarte haben und die Kommunikation zur Durchführung der Authentisierung sowie zur Übertragung der auf der Trägerkarte verschlüsselt abgelegten Befehlssequenz zur Kundenkarte hin unterstützen.

Da gemäß der bevorzugten Ausführungsform die Befehlssequenz bereits verschlüsselt auf der Trägerkarte gespeichert ist, ist selbst bei manipulativem Eingriff in das die Kommunikation herstellenden Terminal eine Betrugsmöglichkeit weitgehend ausgeschlossen, da eine Entschlüsselung der von der Trägerkarte gelieferten Daten sowie ein Zugriff auf die zu programmierende Mikroprozessorkarte nur bei Kenntnis des entsprechenden Schlüssels K möglich ist.

Selbstverständlich muß der Datenträger, der die verschlüsselte Befehlssequenz für die Umprogrammierung enthält, nicht an jeder Stelle, an der die Umprogrammierung der Mikroprozessorkarten möglich ist, körperlich vorhanden sein; die entsprechenden Daten können selbstverständlich auch beispielsweise über eine Modemverbindung von einer zentralen Stelle zu den einzelnen Stellen übertragen werden.

Was oben als Befehlssequenz bezeichnet wurde, kann selbstverständlich nicht nur die eigentlichen Befehle, die der Mikroprozessor für die entsprechende Konfigurierung benötigt, umfassen, sondern auch alle Daten, die für die bestimmte Anwendung erforderlich sind. Derartige Daten können beispielsweise ein Geldguthabendaten, Schlüssel für die Durchführung von Authentisierungsverfahren im Rahmen der zusätzlichen Anwendungen etc. umfassen.

Gemäß der vorliegenden Erfindung werden die Daten gesichert von dem Datenträger bzw. der Trägerkarte zu der zu programmierenden Mikroprozessorkarte übertragen. Die Sicherung erfolgt dabei derart, daß eine Endsicherung innerhalb der zu programmierenden Mikroprozessorkarte mittels eines gespeicherten Schlüssels K möglich ist. Zur Sicherung können nicht nur die üblichen Verschlüsselungsverfahren verwendet werden, sondern auch alle gängigen kryptographischen Verfahren wie beispielsweise elektronische Signatur etc.

Insoweit der Ausdruck "Programmieren" verwendet wurde, soll dieser nicht daraufhin beschränkt verstanden werden, daß eine Programmierung auf Maschinensprachenebene erfolgt. Vielmehr und bevorzugterweise wird die Mikroprozessorkarte mittels höherer Befehle zur Durchführung der Neukonfiguration angesprochen, vorzugsweise mittels Befehlen die durch das Betriebssystem des entsprechenden Mikroprozessors bereitgestellt werden. Die als Befehlssequenz bezeichneten Daten müssen dabei nicht notwendigerweise von dem Mikroprozessor direkt ausführbare Befehlscodes aufweisen, vielmehr besteht die Befehlsequenz allgemein ausgedrückt aus Information, durch die der Mikroprozessor veranlaßt wird, die entsprechende Umkonfiguration vorzunehmen.

Gemäß dem vorliegenden Verfahren kann der auf einer Mikroprozessorkarte für zusätzliche Anwendungen anfänglich zur Verfügung stehende Speicherbereich bytegenau unter beliebigen Anwendungen aufgeteilt werden. Eine Unterteilung des Bereiches in starre Felder, die anschließend u.U. nur unvollständig genutzt werden, wird somit vermieden.

Da mit Hilfe des vorliegenden Verfahrens alle Möglichkeiten des programmierbaren Mikroprozessors genutzt werden können, besteht zusätzlich die Möglichkeit, die Strukturierung der Daten exakt nach den Bedürfnissen der Anwendung durchzuführen bzw. sogar zusätzlichen Programmcode in die Karte einzubringen, der es gestattet, das Verhalten des Mikroprozessors optimal an die neue Anwendung anzupassen.

Gegenüber den bisher bekannten Verfahren weist das vorliegende Verfahren den Vorteil auf, daß die an den Mikroprozessor übermittelte Information nicht mißbräuchlich verwendet werden kann, daß zur Verwendung der übermittelten Information keinerlei Wissen über die bereits auf der Karte gespeicherten Daten benötigt wird, daß die zur Mikroprozessorkarte übermittelte Information nicht manipuliert werden kann bzw. eine Manipulation sicher erkannt wird und schließlich daß die übermittelte Information nur für die dafür vorgesehenen Karten verwendbar ist, da eine Verwendung der übermittelten Information das Vorhandensein des Schlüssels K auf der Karte bedingt.

Patentansprüche

1. Verfahren zum gesicherten nachträglichen Programmieren einer Mikroprozessorkarte für ein zusätzliche Anwendung, mit folgenden Schritten:

   Speichern eines Schlüssels K in einem Speicher der nachträglich zu programmierenden Mikroprozessorkarte,

Erstellen einer Befehlssequenz, mittels der die Mikroprozessorkarte für die zusätzliche Anwendung konfigurierbar ist,

Speichern der verschlüsselten Befehlssequenz auf einem Datenträger, vorzugsweise einer weiteren Mikroprozessorkarte,

Einrichten einer Datenkommunikation zwischen der nachträglich zu programmierenden Mikroprozessorkarte und dem Datenträger bzw. der weiteren Mikroprozessorkarte,

Durchführen eines Authentisierungsverfahrens zum Überprüfen, ob die nachträglich zu programmierende Mikroprozessorkarte für die nachträgliche Programmierung zugelassen ist, und/oder ob der Datenträger bzw. die zusätzliche Mikroprozessorkarte für die nachträgliche Programmierung zugelassen ist,

bei erfolgreichem Abschluß der Authentisierung schrittweises oder vollständiges Übertragen der Befehlssequenz in gesicherter Form von dem Datenträger bzw. der weiteren Mikroprozessorkarte an die nachträglich zu programmierende Mikroprozessorkarte,

Entsichern der empfangenen, gesicherten Befehlssequenz bzw. Befehlssequenzteile durch den Mikroprozessor der zu programmierenden Mikroprozessorkarte mittels des gespeicherten Schlüssels K,

Anlegen von Daten und/oder Programmstrukturen innerhalb eines freien Speicherbereiches der nachträglich zu programmierenden Mikroprozessorkarte entsprechend der Befehlssequenz, wodurch die Mikroprozessorkarte für die zusätzliche Anwendung konfiguriert wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Befehlssequenz bereits in gesicherter Form auf dem Datenträger bzw. der weiteren Mikroprozessorkarte gespeichert wird, derart, daß eine Entsicherung mittels des Schlüssels K möglich ist.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Sicherung mittels kryptographischer Verfahren erfolgt, vorzugsweise mittels geeigneter Verschlüsselungsverfahren.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß in das Authentisierungsverfahren ebenfalls der Schlüssel K einbezogen ist.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß der Schlüssel K während der ersten Personalisierung der Karte gespeichert wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die nachträgliche Programmierung in einem Terminal durchgeführt wird, in das sowohl die zu programmierende Mikroprozessorkarte als auch die weitere Mikroprozessorkarte eingesteckt werden und das die Datenkommunikation zwischen den Karten ermöglicht.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die verschlüsselte Befehlssequenz die für die entsprechende Anwendung notwendigen Daten enthält.

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 97 11 9367

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.6)
X	EP 0 707 290 A (CP8 TRANSAC) * Zusammenfassung; Ansprüche; Abbildung 1 * * Spalte 5, Zeile 16 - Spalte 6, Zeile 42 * ---	1-3,5-7	G07F7/10
A	FR 2 681 165 A (GEMPLUS CARD INTERNATIONAL) * Zusammenfassung; Ansprüche; Abbildungen * ---	1-3,5-7	
A	WO 93 20538 A (TELSTRA CORPORATION) * Zusammenfassung; Ansprüche; Abbildung * ---	1-7	
A	FR 2 536 928 A (ÉTAT FRANCAIS) ---		
A	US 4 855 578 A (K. HIROKAWA) -----		

RECHERCHIERTE SACHGEBIETE (Int.Cl.6)

G07F

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	19.März 1998	David, J

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

DOCID: <EP__0847031A1_I_>